PROCEDURE 1410.20
Issued: January 9, 2001

SUBJECT: Client Firewall Standard

APPLICATION: Executive Branch Departments and sub-units and non-executive branch entities when accessing the State of Michigan data communication networks (LMAN, or SOM-WAN) from any always on or "last mile" shared media connection access.

PURPOSE: To standardize a client firewall (desktop or personal firewall) security policy and guideline for State of Michigan agencies connecting to internal data communications networks from remote locations over a shared media connection such as cable modems, Digital Subscriber Lines (DSL), or earth-orbit satellite "always on" or full access connections.

CONTACT AGENCY: Department of Information Technology (DIT)
Office of Strategic Policy

TELEPHONE: 517/373-7326

FAX: 517/335-2355

SUMMARY:

This procedure establishes the circumstances where the use of client firewall technology commonly referred to as desktop or personal firewalls is mandated by State of Michigan security policy and best practice to protect internal networks, devices, and hosts from external security risks associated with potential Internet-based attacks and hacks.

The applicable transport mechanisms and international standard protocols include:

TCP/IP, PPP, IPv.6.

Applicable Internet Engineering Task Force Request for Comments include:
RFC 2979 "Behavior of and Requirements for Interoperability for Internet Firewalls".
RFC 1775 "To Be "On" the Internet".

APPLICABLE FORMS: None.

PROCEDURES:

General Information:

The objectives of the ***client firewall*** (desktop or personal firewall) ***standard*** are to:

Protect State of Michigan systems from unauthorized access or use.

Improve the overall level of trust inherent in the State of Michigan network infrastructure.

Support the secure remote access needs of the agencies mobile and transient workforce for 24 x 7 access to internal system hosted resources.

Protect internal enterprise and agency hosts from risks associated with negligent security from low-security-profile applications or servers providing the initiation point for launching an attack on high-security-profile applications, devices, and host systems.

Enhance security profile for all enterprise hosts and applications.

Benefits expected:

Accommodate appropriate use of low-cost higher-speed shared media connections to state resources over the Internet or business partner networks.

Increase choices available for selection of local Internet Service Provider (ISP) or Access Service Provider (ASP) **client connections** based on overall best value to the State of Michigan.

Increased security for internal hosts and networks.

Reduction of risks associated with use of shared media on public networks.

Increased efficiency.

Simplified perimeter firewall rules base administration.

Applicability:

Conditions of Application:

This standard applies to non-browser client connection from desktops, laptops, or workstations requiring access to any internal State of Michigan host system, server, or network connected host, when the client connection originates from any type of persistent shared media environment such as cable modems, Digital Subscriber Lines, or satellite connections.

This standard applies to the Extranet client access. Extranet is defined as any State of Michigan to business partner Internet tunnel or direct connection or value added network connection, when one connecting client is outside of the State of Michigan's network and the internal destination host is on any of the State of Michigan's internal host networks.

This standard applies to Internet client access. Internet is defined as any State of Michigan employee, contractor, or partner connection across the public Internet, VPN tunneled, or Internet Service Provider access or through any Access Service Provider where one

connecting client is outside of the State of Michigan trusted network perimeter and the internal destination host is on any of the State of Michigan's internal host networks.

This standard does not cover:

1. Client connections internal to the State of Michigan trusted perimeter networks (LMAN or SOM-WAN).

2. SSL enabled Web browser applications available to the Internet.

3. Intermittent connections made over the public switched telephone network using a plain old telephone (POTS) or integrated services digital network (ISDN) dial-in-connections to the State of Michigan's central modem bank. Specifically when the client connections are randomly assigned IP addresses through Dynamic Host Configuration Protocol, (DHCP), a personal/desktop client firewall security solution will not be required, unless the client desktop is also connected to any shared media connection such as a cable modem or foreign local area network.

Assumption:

Agency remote users are accessing State of Michigan network and server resources with state agency provided client workstations configured, managed, and maintained by agency technical staff. Where employees gain access to State of Michigan network and server resources with personal privately owned equipment only SSL enabled web browser applications available to the Internet are employed for access. Further that these web browser enabled applications utilize application layer security best practices such as user name and password, and/or pin number combinations at a minimum, to reduce risk of unauthorized access leading to inappropriate use.

Implementation considerations:

This standard does not address the total security access needs and is intended to supplement and/or be combined with other security standards and best practices such as two-factor authentication, host user id and password, and application layer security when indicated as necessary to provide adequate risk reduction.

Agencies must coordinate specific remote access needs with Telecom Operations (Network Operations Center) and review security risk threat profile analysis with the Enterprise Security Director.

Technical Considerations: The first implementations of client firewall will standardize on **Symantec Desktop Firewall™ 2.0**. The key fact and feature of this selection include the VPN neutrality of the product, its frequent bundling with cable modem products and compatibility with Windows 95/98 and Windows 2000 desktop operating systems. This product is currently available on the State of Michigan Master Contract.

Maintenance:

DMB: Acquisition Services shall not approve any acquisition or purchase request without confirmation from the Department of Information Technology, Office of Strategic Policy that such request is in compliance with the standard.

Operational Unit: Any and all projects, consulting requests, equipment and software acquisition requests, or ITB's relating to client, desktop, or personal firewall will be subject to review for compliance with this standard.

DIT: The Office of Strategic Policy will review this standard on a continuing basis and make recommendations for changes. An appropriate group of staff, representing a wide-range of State Operational Units, will review and possibly revise these standards and guidelines as often as needed.

Exceptions from this standard for reasons other than those outlined above will be made through the exception handling process described in the Exception Process Template.

***